EXHIBIT
M

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a
California Corporation,

Plaintiff,

vs. Case No. 04-1199-SLR

INTERNET SECURITY SYSTEMS,
INC., a Delaware
corporation, INTERNET
SECURITY SYSTEMS, INC., a
Georgia corporation, and
SYMANTEC CORPORATION, a
Delaware corporation,

Defendants.
_______________________________/

Deposition of
FREDERICK M. AVOLIO
May 18, 2006

Reported by
John Wissenbach, CSR 6862

SHARI MOSS & ASSOCIATES
Certified Shorthand Reporters
110 Sutter Street, Suite 607
San Francisco, California 94104
(415) 402-0004
(650) 692-8900
FAX: (415) 402-0005

that's mentioned here, "Firewalls and Internet Security." Also, Chapman and Zwicky's book mention that as being part of what makes up a firewall: the ability to log and keep track of -- of data.

Q. Would you agree that as of 1998, that some firewalls did not have logging capabilities?

MS. BROWN: Objection; vague.

THE WITNESS: All firewalls that -- well, some value of "all." All the major firewalls at the time did some logging. It was a requirement of any security system to have logging.

In fact, most of the firewalls at the time -- most of the firewalls at the time routinely and somewhat automatically did logging, in that most of them were built on some version of Berkeley UNIX using the syslog utility. It was a standard utility for years before that time period. It was just something that software developers used when developing software on UNIX systems. It was also something that was standard on firewalls. It was a requirement to have logging on a firewall.

BY MR. POLLACK:

Q. So would it be your opinion that all firewalls that existed in 1998 all had logging capability?

MS. BROWN: Objection; vague, calls for speculation.

THE WITNESS: Certainly not all, because "all firewalls" include the simplest router. Today the simplest firewalls, on home systems, for example, or on a Windows PC or on a Macintosh, do some kind of logging. All do. I'm sure there -- I shouldn't say I'm sure. I suppose there might have been firewalls that did not do logging. But that was a requirement of -- of -- of firewalls at the time.

BY MR. POLLACK:

Q. Would you also agree that in -- as of 1998, the logging facilities that were provided varied fairly considerably among the different products offered by vendors?

MS. BROWN: Objection; vague.

THE WITNESS: I -- I wouldn't be able to -- I know logging was a differentiator, and what was logged. But I don't know how -- you said varied considerably. I don't know if I would say that. I -- I couldn't say that.

BY MR. POLLACK:

Q. You don't recall having said that before?

A. I certainly recall having said in

particular field at all; just like earlier in the document, I said audit logs are logs. Auditors care about the word "audit." But they're used interchangeably routinely. They were back in the early nineties. They are today.

BY MR. POLLACK:

Q. So it's your belief, then, that there are lots of different kinds of activity logs, and one of which would be a firewall log, would be an example?

A. I would say that firewall logs can be characterized as activity logs.

Q. Would you say that other things could be characterized as activity logs?

MS. BROWN: Objection; calls for speculation, incomplete hypothetical.

THE WITNESS: Well, yeah. On my PowerBook, the PowerBook logs activities, not all of which is related to firewalls. So "activity log" is a more general term, which includes firewall logs, or which may include firewall logs.

BY MR. POLLACK:

Q. And would the same be true for application logs, that it's a more general term that may include firewall logs but would include other types of applications as well?

MS. BROWN: Objection; vague.

THE WITNESS: Could.

BY MR. POLLACK:

Q. I'll refer you to page 22 of your report, paragraph 67.

A. Yes.

Q. You state that "firewall configuration requires one to set the firewall to monitor," and then paren 1, "network connection requests for packets that will be allowed to pass through the firewall," quote, "'pass-through traffic.'"

Why -- why is it that you believe that the firewall has to monitor network connection requests to decide whether or not to pass through a packet?

MS. BROWN: Objection; vague.

THE WITNESS: Well, I believe it's true. And in Garfinkel and Spafford, they point that out. In -- I mean, that's one of the basic -- well, let me see. I'm reading your question again.

A network connection request is required before a firewall can look at a packet at all. So by definition it has to recognize network connection requests. Firewalls monitor those such things.

BY MR. POLLACK:

Q. Is it your opinion that firewalls base

Q. So is it your opinion that in 1997, 1998, vendors would be recommending that users of their products log everything that the firewall was capable of logging?

MS. BROWN: Objection; calls for speculation, lacks foundation.

THE WITNESS: No, and in particular they didn't recommend that. But -- but firewalls did log connections. That was less a part of the firewall particular function and more a function of the network kernel in the -- in BSD UNIX and in other versions of -- of UNIX at the time.

BY MR. POLLACK:

Q. Isn't it true that there were practical limitations in the 1998 time frame as to what one could log without detracting from the performance of the firewall?

MS. BROWN: Objection; lacks foundation, calls for speculation.

THE WITNESS: There's always going to be -- yes. Sure.

BY MR. POLLACK:

Q. And so it's true that one would have to apply some thought and analysis to the types of information that they believed was appropriate and practical to log in any particular environment, correct?

A. Yes. The -- yes, that's correct. Most -- the firewalls that used Berkeley UNIX foundations did log network connections, because the Berkeley kernel logged network connections. Firewalls -- other firewalls, that are mentioned in the ICSA Labs buyer's guide -- there's a -- there was a list of things that ought to be logged, should be logged, and, by reference, some of the things that firewalls at the time did log, in the paper, the report.

MS. BROWN: Do you think we could maybe take a quick break now?

MR. POLLACK: Sure.

We're going to go off the record and take a ten-minute break.

THE VIDEOGRAPHER: This marks the end of tape number 1 in the deposition of Frederick M. Avolio. Going off the record, the time is 10:56 a.m.

(Recess taken.)

THE VIDEOGRAPHER: Going back on the record, the time is 11:04 a.m.

BY MR. POLLACK:

Q. Referring you a little further in your